Exhibit A

Exhibit A

Plaintiffs Evgeniy Goussev ("Goussev") and Stacy Ritch ("Ritch," and collectively "Plaintiffs"), individually and on behalf of all others similarly situated, allege the following based upon personal knowledge as to Plaintiffs and Plaintiffs' own acts, and upon information and belief as to all other allegations, based on investigation of counsel. This investigation included, *inter ~~alia~~ alia*, a review of public documents prepared by Defendant, media reports, and other information concerning Defendant, as well as information from and concerning Berla Corporation. The investigation of the facts pertaining to this case is continuing. Plaintiffs believe that substantial evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

I. INTRODUCTION

1. This class action suit seeks statutory damages for violations of the Washington Privacy Act, Chapter 9.73 RCW (hereafter the "WPA" or the "Act"), which forbids any entity ~~in Washington~~ from intercepting or recording any private communication in the State of Washington without first obtaining the consent of all the participants in the communication.[1]

2. Because Defendant has violated the WPA, it is liable for liquidated damages computed at the rate of one hundred dollars per day for each day of violation, not to exceed one thousand dollars per Plaintiff and absent class member, and a reasonable attorneys' fee and other costs of litigation.

3. Plaintiffs are also entitled to declaratory and injunctive relief that Defendant has violated the WPA, and enjoining further violations.

II. JURISDICTION AND VENUE

4. ~~This~~The Thurston County Superior Court has jurisdiction over the subject matter of this lawsuit and over the parties to the lawsuit.

5. Venue is proper in ~~this~~the Thurston County Superior Court pursuant to RCW 4.12.025 because Defendant resides in ~~this~~ Thurston ~~c~~County.

III. PARTIES

[1] As described below, Plaintiffs seek to represent a class consisting of: "All persons, who in the three years prior to the date of filing this Complaint~~;~~, had their text messages and/or call logs intercepted and/or recorded by the infotainment system in a Toyota vehicle (Toyota or Lexus) while a resident of the State of Washington.~~))~~"

6. Plaintiff Goussev is now, and at all times relevant to this Complaint has been, a Washington resident.

7. Plaintiff Ritch is now, and at all times relevant to this Complaint has been, a Washington resident.

8. Defendant Toyota Motor Sales, U.S.A., Inc. is a wholly-owned subsidiary of Toyota Motor Corporation, a publicly held Japanese automotive manufacturer headquartered in Toyota City, Japan. Assisted by its subsidiaries and affiliates worldwide, Toyota Motor Corporation designs, manufactures, assembles, and sells "Toyota" and "Lexus" brand vehicles. ~~Together herein, these vehicles are referred to as "Toyota vehicles" or "vehicles manufactured by Toyota."~~

9. Toyota Motor Sales, U.S.A., Inc. (hereafter, "Toyota") is headquartered in Plano, Texas, and is ~~re_sponsible~~responsible for the marketing, sales, and distribution in the United States of Toyota vehicles. Together herein, these vehicles are referred to as "Toyota vehicles" or "vehicles manufactured by Toyota."

IV. FACTS

A. Toyota vehicle infotainment systems.

10. Modern vehicles, including ~~those built~~vehicles manufactured by Toyota, contain "infotainment systems."

11. Infotainment systems in Toyota vehicles include methods for the system to connect to a smartphone, both by USB and by Bluetooth.

12. Once a smartphone is connected to the infotainment system in a Toyota vehicle, the system offers additional apps and functionality native to the smartphone but controlled and accessed through the infotainment system controls rather than through the smartphone.

13. These can include, for example, the ability to play music stored on or streamed through the smartphone through the vehicle's speakers, and to use the smartphone's satellite navigation software through the infotainment system screen and vehicle speakers for turn-by-turn directions.

14. Infotainment systems in Toyota vehicles also include the ability to make and receive telephone calls on a connected smartphone, using the vehicle microphone and speakers and thereby operating hands-free.

15. At all relevant times, infotainment systems in Toyota vehicles also interface with the smartphone's text messaging system.

16. ~~The interface of infotainment~~Infotainment systems in Toyota vehicles ~~is~~are designed to work specifically with at least the two major smartphone operating systems: CarPlay for Apple smartphones (iPhones) and Android Auto for Android smartphones.

17. ~~On information and belief, infotainment~~Infotainment systems in Toyota vehicles ~~manufactured~~ from at least 2014 onward ~~also~~automatically and without authorization, record, download ~~and~~, store, and are capable of transmitting, a copy of all text messages already stored on smartphones when ~~connected~~those phones connect to ~~Toyota's~~the infotainment system~~s~~.

18. ~~On information and belief, third~~Infotainment systems in Toyota vehicles from at least 2014 onward automatically and without authorization, instantaneously intercept, record, download, store, and are capable of transmitting, a copy of all text messages sent from or received by a smartphone while the smartphone is connected to the infotainment system.

19. Toyota vehicles store each intercepted, recorded, and downloaded copy of text messages in non-temporary computer memory in such a manner that the vehicle owner cannot access it or delete it.

20. Even if the text message is deleted from the smartphone, the Toyota vehicle retains a copy in on-board memory, even after the smartphone is disconnected.

21. Infotainment systems in Toyota vehicles from at least 2014 onward automatically and without authorization, record, download, store, and are capable of transmitting, a copy of all records of incoming and outgoing calls and call durations ("call logs") already stored on smartphones when those phones connect to the infotainment system.

22. Infotainment systems in Toyota vehicles from at least 2014 onward automatically and without authorization, instantaneously intercept, record, download, and store a copy of all call logs of calls sent from or received by a smartphone while it is connected to the infotainment system.

23. Toyota vehicles store each intercepted, recorded, and downloaded copy of call logs in non-temporary computer memory in such a manner that the vehicle owner cannot access it or delete it.

24. Even if the call logs are deleted from the smartphone, the Toyota vehicle retains a copy in on-board memory, even after the smartphone is disconnected.

25. Third party Berla Corporation ("Berla"), based in Annapolis, Maryland, manufactures equipment (hardware and software) capable of extracting stored text messages from infotainment systems in Toyota vehicles.

~~19. On information and belief, the~~

26. Berla also manufactures equipment capable of extracting stored call logs from infotainment systems in Toyota vehicles.

27. Toyota infotainment systems thereby transmit stored text messages and call logs to Berla.

28. The functions described in paragraphs 17-27 above, are not necessary to enable Toyota infotainment systems to perform the functions of making and receiving calls or text messages, but are superfluous features used only to surveil by unauthorized third parties.

29. The functions described in paragraphs 17-27 above, are not necessary to enable Toyota infotainment systems to comply with law or regulation, but are superfluous features used only to surveil by unauthorized third parties.

30. The Berla system is not generally available to the ~~general~~ public.

~~20.~~

31. Even when smartphone users restrict access to their data on the phone by a password, fingerprint, face image, or other security method, the text message and call log data copied onto the vehicle can be, and is, transmitted to users of Berla's equipment without requiring any kind of password, biometric, or other security measure.

32. Berla states that "Our vehicle forensics tools are available to law enforcement, military, civil and regulatory agencies, and select private industry organizations."[2]

~~21. On information and belief, infotainment systems in Toyota vehicles automatically download a copy of every text message stored on any phone connected to the system and stores that copy in computer memory on the vehicle in such a manner that the vehicle owner cannot access it.~~

~~22~~

33. According to Berla, while a vehicle owner cannot retrieve text messages stored on Toyota vehicles, Berla and Toyota have ensured that unauthorized law enforcement can.

34. ~~However, according~~According to Berla, while a vehicle owner cannot retrieve ~~that text message~~the call logs stored on the Toyota vehicle, Berla and Toyota have ensured that unauthorized law enforcement can.

~~23~~35. According to a 2017 report in CyberScoop, Ben LeMere, the CEO and founder of Berla, bragged in 2014 that "We've been working directly with the [original equipment manufacturers] themselves to educate them. Hey, 'this is privacy data,' 'this is what you need to secure.' ***But we only do that when it's part of an agreement that they will allow ~~la,v~~law enforcement in.***"[3] (Emphasis added.)

~~24. In a~~

36. In other words, copies of text messages and call logs stored on Toyota vehicles can be, and are, retrieved by unauthorized users of Berla's equipment without any password, fingerprint, face image, or other security measures, thus bypassing any security measures Plaintiffs and class members employ to secure data on their phones.

37. According to Berla, beginning no later than 2014, vehicle manufacturers including manufacturers of Toyota vehicles, worked with Berla to ensure that vehicle infotainment systems would copy and store text messages and call logs without authorization, in such a manner that vehicle owners

[2] *See* https://berla.co/ (last accessed May 24, 2021).

[3] *See* https://www.cyberscoop.com/berla-car-hacking-dhs/ (last accessed ~~May 24~~November 4, 2021~~ and attached hereto as Exhibit A~~). That article refers to, and quotes, a 19:52 minute presentation found at https://www.youtube.com/watch?v=~~EODQEVgfYSk~~E0DQEVgJY5k.

could not delete them, to ensure such data remains available for unauthorized retrieval by law enforcement.

38. As early as February 9, 2015, Berla described that "hybrid" navigation devices, those that connected to smartphones, "will generally have call logs (incoming/outgoing and missed), an address book (which is normally imported from the mobile phone), the MAC address of the last ten mobile phones connected to it, and sent and received SMS messages."[4]

39. On March 4, 2015, Berla invited prospective attendees to a "Vehicle Forensics Presentation in Australia," "focused on the vast amount of user data that can be acquired from vehicles. Data such as recent destinations, favorite locations, ***call logs***, contact lists, ***SMS messages***, emails, pictures, videos, social media feeds, and the navigation history of everywhere the vehicle has been." (Emphasis added.)[5]

40. Also beginning no later than April 20, 2015, Berla made publicly available on its website a vehicle lookup feature, which "can be used to find detailed information on North America vehicles between 1981 and the current model year."[6]

41. Berla's vehicle lookup tool allows a user to input a VIN and receive back a report of exactly what information that vehicle stores which can be retrieved by the Berla system.

42. Berla's vehicle lookup system is no longer publicly available. Berla's website states that instead, "Access is now limited to iVe Mobile and the iVe Software. However, iVe Mobile is available at no cost, to law enforcement, military, civil and regulatory agencies, and select private industry organizations."[7]

43. As early as May 15, 2015, Berla's system "support[ed] the majority of 2012 and newer Toyota vehicles."[8]

[4] *See* https://berla.co/enhancing-investigations-with-gps-evidence/ (last accessed November 4, 2021).
[5] *See* https://berla.co/invitation-vehicle-forensics-presentation-in-australia/ (last accessed November 4, 2021).
[6] *See* https://berla.co/ive-v1-6-released/ (last accessed November 4, 2021).
[7] *See* https://berla.co/vehiclelookup/ (last accessed November 4, 2021).
[8] *See* https://berla.co/toyota-entune-systems/ (last accessed November 4, 2021).

44. On March 12, 2019, Berla announced the release of v2.3, which "adds support for a considerable number of Lexus vehicles manufactured between 2010 and 2016 . . ."[9]

45. On or about January 31, 2021, Berla's system "add[ed] support for additional Toyota vehicles, the majority of which fall between 2014-2015."[10]

46. On or about August 28, 2020, Berla's system "[a]dded support for Toyota hard drive systems manufactured from 2012-2015."[11]

47. Toyota vehicles store unauthorized call logs and SMS messages of phones which had been connected to it, as alleged above, capable of being retrieved by unauthorized third parties using Berla equipment.

48. Berla's July 22, 2015 release also "[a]dded [a] feature to decode non-US Vehicle Identification Numbers (VINs)", and reminded users that "you can always use the vehicle lookup tool on our website to see if a vehicle is supported."[12]

49. Beginning at least as early as 2015, Berla confirmed that ordinary users of vehicle infotainment systems were largely unaware of the extent to which private data was intercepted, copied, recorded, downloaded, and stored by vehicle infotainment systems.

50. In a September 17, 2015 blog post, Berla embedded an article co-authored by its founder, Ben LeMere, emphasizing that "it is incredibly likely that investigators are missing out on digital evidence that could make or break their cases."[13] The article specifically listed call logs and SMS data as among the data stored on infotainment systems such as those installed on Plaintiffs and class member vehicles by Toyota.

51. In a December 13, 2015 blog post, Berla embedded and commented favorably on an article published in the "Minnesota Police Journal," "The Official Publication of The Minnesota Police and Peace Officers Association," stating "Berla has always made it a priority to support Law Enforcement officers, and it is a great validation when one sees the value of our work and takes

[9] *See* https://berla.co/ive-software-v2-3-release/ (last accessed November 4, 2021).
[10] *See* https://berla.co/ive-software-v2-6-release/ (last accessed November 4, 2021).
[11] *See* https://berla.co/ive-software-v3-0-release/ (last accessed November 4, 2021).
[12] *See* https://berla.co/ive-v17/ (last accessed November 4, 2021).
[13] *See* https://berla.co/berla-in-uslaw-magazine/ (last accessed November 4, 2021).

the initiative to share it within one's own professional community. In this case, it is the Minnesota Police & Peace Officers Association (MMPOA)."[14]

52. The author, a retired St. Paul, MN police sergeant, described how a colleague synced his smartphone to a rental car the two were in.[15] The author wrote: "By syncing his phone to this vehicle, all of his phone book names and numbers, call lists, call history, cell phone model and type, cell name, SMS text messages, social media, emails, and dozens of other bits of information had now been copied to the memory of the vehicles infotainment system. Depending on the configuration of the phone and Infotainment system, this could also include recent destinations, and navigation history. 'It does that? No (expletive)?' was his reply."[16]

53. On December 29, 2015, Berla posted "12 Days of Vehicle Forensics," a collection of 12 facts about vehicle forensics[17]

54. These facts included that "Connecting a smartphone to a car via USB just to charge will still result in some phone data being stored on the infotainment system."[18]

55. These facts included that "OEMs decide what OS and hardware to use, and implement that setup into all brands. As such, vehicle forensic support is global — the same tool is used regardless of country."[19]

56. These facts included that "If a driver uses the infotainment interface to 'delete' their device, that device information often remains in unallocated space and can be recovered."[20]

57. These facts included that "Having access to a suspect's connected vehicle is the next best thing behind having the actual phone itself."[21]

[14] *See* https://berla.co/berla-in-minnesota-police-siu-publication/ (last accessed November 4, 2021).
[15] See https://berla.co/wp-content/uploads/2016/01/MPPOAOct2015.pdf (last accessed November 4, 2021).
[16] *Id.*
[17] *See* https://berla.co/12-days-of-vehicle-forensics/ (last accessed November 4, 2021).
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.*

58. These facts included that "Data can remain on a vehicle's system for weeks, months or even years."[22]

59. Since at least December 2015 and continuing to today, Toyota vehicle infotainment systems intercept, record, download and store an unnecessary, and unauthorized copy of phone data, including text messages and call logs, from phones connected, even merely to charge. Toyota vehicles continue to store deleted data in a manner such that it can be retrieved by Berla equipment, and such data remains on Toyota vehicle systems for weeks, months, or even years solely for the purpose of unauthorized surveillance by third parties.

60. In a blog post dated January 19, 2016, Berla noted that it had added a feature to its publicly-available VIN-based vehicle lookup tool: "As a reminder, you can always use the vehicle lookup tool on our website to see if a vehicle is supported as we are constantly adding to it. In fact, we just added a feature that displays ***what data can be extracted from each vehicle***."[23] (Emphasis added.)

61. Since at least January 2016 and continuing to today, Berla's lookup tool reports, by VIN, what data can be extracted from each Toyota vehicle.

62. On February 22, 2016, Berla touted its receipt of a Department of Homeland Security "Significant Government Impact Award." It noted that "Frequently motor vehicles are used in the commission of crimes and may include valuable digital evidence. This evidence can often be instrumental to law enforcement in a criminal investigation, just like a computer or cell phone. Data of interest is normally stored inside a vehicle's infotainment and telematics system. Vehicle infotainment and telematics systems store a vast amount of data such as recent destinations, favorite locations, ***call logs***, contact lists, ***SMS messages***, emails, pictures, videos, social media feeds, and the navigation history of everywhere the vehicle has been."[24] (Emphasis added.)

---

[22] *Id.*

[23] *See* https://berla.co/ive-v1-8-released-and-ive-mobile/ (last accessed November 4, 2021).

[24] *See* https://berla.co/berla-corporation-and-project-ive-receive-significant-government-impact-award/ (last accessed November 4, 2021).

63. Since at least February 2016, and continuing to today, Toyota vehicle infotainment systems automatically intercept, record, download, store, and are capable of unauthorized transmittal of call logs and text messages to Berla and law enforcement.

64. On September 28, 2016, Berla invited attendees to vehicle forensics presentations to learn "how to acquire and analyze the data" stored on vehicles, including "call logs [and] SMS messages . . ."[25]

65. Since at least September 2016 and continuing to today, owners of Berla equipment can, and do, retrieve without authorization, the call logs and text messages of smartphones which have been connected to Toyota vehicles.

66. On November 9, 2016, Berla announced a partnership with Stockholm-based MSAB (a company which later contracted with the United States Customs and Border Patrol to make Berla equipment available to retrieve data from any vehicle encountering a Border Patrol agent). Berla reiterated that its iVe system "provides forensic examiners and investigators a means to quickly and intuitively acquire and analyze data from vehicle systems. Vehicle systems store a vast amount of data such as recent destinations, favorite locations, call logs, contact lists, SMS messages, emails, pictures, videos, social media feeds, and the navigation history of everywhere the vehicle has been."[26]

67. Since at least 2016 and continuing today, through use of Berla's iVe system, unauthorized third parties can and do acquire call logs and text messages from Toyota vehicles.

68. In a blog post dated January 16, 2017, Berla revealed a new visual format for presenting data extracted from vehicles, explicitly including call logs.[27]

69. Since at least 2017 and continuing to today, Toyota vehicle infotainment systems retain unauthorized copies of call logs from connected smartphones which can be, and are, retrieved by unauthorized third parties using Berla equipment.

[25] *See* https://berla.co/join-us-on-the-fall-forensic-world-tour/ (last accessed November 4, 2021).
[26] *See* https://berla.co/berla-and-msab-announce-strategic-partnership/ (last accessed November 4, 2021).
[27] *See* https://berla.co/ive-v1-10-released/ (last accessed November 4, 2021).

70. In that same post, Berla confirmed that it "Added 'Flags' column for SMS messages to show deleted", confirming that its system retrieves text messages users deleted on their phones but which the infotainment system retains without authorization.

71. Since at least 2017 and continuing to today, Toyota vehicle infotainment systems retain unauthorized copies of text messages which users deleted from their smartphones, which can be, and are, retrieved by unauthorized third parties using Berla equipment.

72. In a May 22, 2017 blog post, Berla stated that "Whenever a mobile device is connected to a vehicle system via USB, Bluetooth, or Wi-Fi, some data from that device is stored in the vehicle. Potentially, device contacts, call logs, and SMS messages are stored and can thus be acquired in iVe . . ."[28]

73. Since at least 2017 and continuing today, Toyota vehicles store an unauthorized copy of call logs and text messages from mobile devices connected to Toyota vehicle systems via USB, Bluetooth, or Wi-Fi, which can be, and are, retrieved by unauthorized third parties using Berla equipment and systems.

74. On September 11, 2017, reporter Patrick O'Neill wrote that, in the San Bernadino terrorism investigation, while Apple refused to build a "backdoor" for access to a suspect's iPhone, Berla touted that its equipment evaded any security protections from the suspect's iPhone, with LeMere specifically stating that "We've assisted in pretty much every major terrorism investigation in the last year, from the Paris bombing to the Chattanooga, Tennessee, shooting to San Bernardino".[29] The image embedded in that article, a screen shot of the iVe system, specifically shows that the iVe system can retrieve call logs and SMS messages.

75. On April 4, 2018, Berla posted a description of the "Value of Vehicle System Data in Accident Reconstruction."[30] In that post, it reiterated that, in addition to federally defined "event data," vehicles also record information from "synced devices, phone calls, and text messages". It continued, "That data may be recorded in the vehicle's infotainment and telematics system, along

[28] *See* https://berla.co/exporting-xry/ (last accessed November 4, 2021).
[29] *See* https://www.cyberscoop.com/berla-car-hacking-dhs/ (last accessed November 4, 2021).
[30] *See* https://berla.co/vehicle-system-data-and-accident-reconstruction/ (last accessed November 4, 2021).

with whether or not a particular person's cell phone was used in the car, ***what calls were made, and/or what text messages were sent***. In some instances, the actual audio recording of an occupant using the voice recognition system may be stored. The above types of data cannot simply be obtained through a basic OBD-II port hookup and the press of a button, but iVe is a tool that facilitates the acquisition of data from many infotainment and telematics systems."

76. Since at least at least April 4, 2018 and continuing to today, Toyota infotainment systems intercept and record call logs and text messages from phones connected to those infotainment systems, and store those logs and messages for retrieval by unauthorized third parties using Berla iVe systems.

77. On August 28, 2020, Berla announced a new release of its iVe software.[31] That post showed an exemplary set of vehicle data, by VIN, including call logs intercepted, recorded, copied and stored from an iPhone 12.

78. For at least the three years prior to the filing of the initial complaint in this matter, Toyota vehicles have intercepted, recorded, and stored information protected by the Washington Privacy Act, including text messages and call logs, without the consent of users, while bypassing any password or biometric security that users include on smartphones.

79. For at least the three years prior to the filing of the initial complaint in this matter, Toyota vehicles have stored text messages and call logs intercepted, recorded, and copied from connected smartphones even where such text messages and call logs have been deleted from the smartphone by the user.

80. Such data has been stored on Toyota vehicles in a manner that it can be retrieved by unauthorized third parties using Berla systems.

81. In a December 28, 2020 story published by NBC News, NBC quoted LeMere from a podcast as follows: "'People rent cars and go do things with them and don't even think about the places they are going and what the car records,' LeMere said in a June interview for a podcast made by Cellebrite, a company that makes tools to help law enforcement agencies extract data from

[31] *See* https://berla.co/ive-feature-spotlight-3-0-accessible-collections/ (last accessed November 4, 2021).

locked mobile phones. 'Most of them aren't doing anything wrong, but it's pretty funny to see the hookers and blow request text messages and answers.'[4]

25[82]. A recent[May 3, 2021] article published by The Intercept quoted LeMere as follows: "In a 2015 appearance on the podcast 'The Forensic Lunch,' LeMere told the show's hosts how the company uses exactly this accidental-transfer scenario in its trainings: 'Your phone died, you're gonna get in the car, plug it in, and there's going to be this nice convenient USB port for you. When you plug it into this USB port, it's going to charge your phone, absolutely. And as soon as it powers up, it's going to start sucking all your data down into the car.'[5]

26[83]. The Intercept article continues: "In the same podcast, LeMere also recounted the company pulling data from a car rented at BWI Marshall Airport outside Washington, D.C.: 'We had a Ford Explorer . . . we pulled the system out, and we recovered 70 phones that had been connected to it. All of their call logs, their contacts and their SMS history, as well as their music preferences, songs that were on their device, and some of their Facebook and Twitter things as well . . . And it's quite comical when you sit back and read some of the the [sic] text messages.'[6]

27. On information and belief, a reasonable opportunity for discovery will show that infotainment systems in Toyota vehicles automatically download a copy of all text messages from connected smartphones and store them in onboard computer memory.

28. On information and belief, a reasonable opportunity for discovery will show that the onboard stored copy of text messages cannot be accessed by vehicle owners.

29. On information and belief, a reasonable opportunity for discovery will show that the

---

[4][32] *See* https://www.nbcnews.com/tech/tech-news/snitches-wheels-police-turn-car-data-destroy-suspects-alibis-nl25l939n1251939 (last accessed May 24November 4, 2021 and attached as Exhibit B). That article purports to hyperlink to a podcast at https://www.cellebrite.com/en/series/vehicle-data-extractions-ben-lemere-ceo-at-berla-vehicle-forensics/ but no such pod castpodcast appears at that URL as of May 24, 2021.

[5][33] *See* https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/ (last accessed May 24November 4, 2021 and attached as Exhibit C),. The article contains no internal link to this referenced podcast.

[6] *Id.*

[34] *Id.*

84. The onboard stored copy of text messages can be accessed by someone using hardware and software designed and sold by Berla.

~~30~~85. Berla specifically restricts access to its systems, making them available primarily to law enforcement and private investigation service providers.

~~31~~86. No Plaintiff is able to acquire a Berla system in order to be able to access the text messages stored on his own or any other Toyota vehicle.

87. No Plaintiff is able to acquire a Berla system in order to be able to access the call logs stored on his own or any other Toyota vehicle.

88. The onboard stored copy of call logs cannot be accessed by vehicle owners.

89. Berla specifically restricts access to its systems, making them available primarily to law enforcement and private investigation service providers.

B. Plaintiff Goussev's Toyota infotainment system, ~~smart~~phone, ~~and~~ text messages, and call logs.

~~32~~90. Plaintiff Goussev owns a ~~2019~~2015 vehicle manufactured by Toyota.

~~33~~91. Plaintiff Goussev's Toyota vehicle is equipped with an infotainment system that syncs to any smartphone either plugged into the system through a USB cable or connected via Bluetooth.

~~34~~92. Plaintiff Goussev owns a smartphone.

~~35~~

93. Plaintiff Goussev protects the data on his smartphone with password and biometric security measures.

94. The infotainment ~~sy tem~~system on Plaintiff Goussev's Toyota is a device designed to intercept, record and/ or transmit text communications.

~~36~~95. ~~In~~On at least ten occasions in the past three years, ~~on more than ten occasions~~while in the State of Washington, Plaintiff Goussev connected his smartphone into the infotainment system in his Toyota vehicle~~'s~~ at a time that it had at least one text message stored on it.

96. On at least ten occasions in the past three years, while in the State of Washington, Plaintiff Goussev sent and/ or received a text message while his smartphone was connected to his Toyota vehicle infotainment system.

~~37~~

97. On at least ten occasions in the past three years, while in the State of Washington, Plaintiff Goussev connected his smartphone to his Toyota vehicle infotainment system at a time that it had at least one record of a call he had placed or received.

98. On at least ten occasions in the past three years, while in the State of Washington, Plaintiff Goussev placed and/ or received a call while his smartphone was connected to his Toyota vehicle infotainment system.

99. Plaintiff Goussev never consented to Toyota intercepting, recording, downloading and storing his text messages or call logs, and similarly did not consent to third parties such as Berla or law enforcement having access to copies of such text messages or call logs made by his Toyota ~~vehicle's~~ infotainment system.

~~38. On at least ten occasions in the past three years, Plaintiff Goussev connected his smartphone to his Toyota vehicle's infotainment system at a time that it had at least one text message stored on it.~~

~~39~~

100. Each of Plaintiff Goussev's text messages and call logs was and is a private communication, inasmuch as Plaintiff Goussev had not shared the messages or logs with anyone other than the recipients.

~~40~~101. ~~On information and belief, a reasonable opportunity for discovery will show that each~~Each text message stored on, sent by and received at Plaintiff Goussev's smartphone was downloaded and recorded onto onboard vehicle memory by his Toyota vehicle's infotainment system.

~~41~~

102. Each call log stored on, or generated while a call was placed by or received at Plaintiff Goussev's smartphone was intercepted, downloaded and recorded onto onboard vehicle memory by his Toyota vehicle's infotainment system.

103. Toyota was not a party to any of the text messages or calls.

~~42~~104. By the foregoing conduct, Toyota intercepted and/ or recorded ~~the~~Plaintiff Goussev's text messages and call logs through the infotainment system.

~~43~~105. ~~On information and belief, a reasonable opportunity for discovery will show that~~ Plaintiff Goussev's Toyota vehicle infotainment system wrongfully retains the recorded copy of Plaintiff Goussev's text ~~message~~messages and call logs for more than ten days.

C. Plaintiff Ritch's text messages.

~~44~~106. In the past three years, while in the State of Washington, Plaintiff Ritch sent at least one text message to Plaintiff Goussev.

~~45~~107. Plaintiff Goussev thereafter connected his smartphone to the infotainment system in his Toyota vehicle.

~~46~~108. On information and belief, a reasonable opportunity for discovery will show that Plaintiff Ritch's text message(s) to Plaintiff Goussev ~~was~~were downloaded and recorded onto onboard vehicle memory by Plaintiff Goussev' s Toyota vehicle infotainment system.

~~47~~109. Toyota was not a party to the text message(s).

~~48~~110. By the foregoing conduct, Toyota intercepted and recorded the text messages through the infotainment system.

~~49~~111. On information and belief, a reasonable opportunity for discovery will show that Plaintiff Goussev's Toyota vehicle infotainment system wrongfully retains the recorded copy of Plaintiff Ritch's text message for more than ten days.

D. Privacy of text messages and call logs; Non-consent to Toyota's interception and recording.

~~50~~112. Each of Plaintiff Goussev's text messages and call logs is a private communication between Plaintiff Goussev and his interlocutor.

~~51~~113. Plaintiff Goussev has never consented to Toyota intercepting his text messages or call logs.

~~52~~114. Plaintiff Goussev has never consented to Toyota recording his text messages or call logs.

~~53~~115. Plaintiff Goussev has never inquired of an interlocutor to his text messages whether the counterparty consents to Toyota intercepting and recording the text messages.

~~54~~116. As such, no interlocutor of Plaintiff Goussev has ever consented to Toyota intercepting and/ or recording their text messages.

~~55~~117. Toyota's intercepting and recording of Plaintiff Goussev's text messages and call logs has injured Plaintiff Goussev in his person. ~~On information and belief,~~ Plaintiff Goussev's private and confidential text messages and call logs now reside on his Toyota vehicle, can be accessed without his authorization by Berla systems, and cannot be deleted by Plaintiff Goussev. Each of Plaintiff Goussev's private and confidential text messages and call logs is accessible at any time by law enforcement, by Berla, and by similar private actors without his authorization.

~~56~~118. Toyota has also injured Plaintiff Goussev in his person by depriving him of the right and ability to engage in private phone calls and text communications without ~~unwillingly allowing~~ Toyota ~~to intercept~~intercepting and ~~record a~~recording a call log or text message copy for access by third parties such as Berla and law enforcement, without his authorization.

~~57~~119. Each of Plaintiff Ritch's~~s~~ text messages is a private communication between Plaintiff Ritch and his interlocutor.

~~58~~120. Plaintiff Ritch has never consented to Toyota intercepting his text messages.

~~59~~121. Plaintiff Ritch has never consented to Toyota recording his text messages.

~~60~~122. Toyota's recording of Plaintiff Ritch's text messages has injured Plaintiff Ritch in his person. On information and belief, Plaintiff Ritch's private and confidential text messages now reside on Plaintiff Goussev's Toyota vehicle, and can be accessed without his authorization by Berla systems, and cannot be deleted by either Plaintiff Goussev or Ritch. Each of Plaintiff Ritch's~~s~~ private and confidential text messages to Plaintiff Goussev is accessible at any time by law enforcement, by Berla, and by similar private actors without his authorization.

~~61~~123. Toyota has injured Plaintiff Ritch in his person by depriving him of the right and ability to engage in private text communications without ~~unwillingly allowing~~ Toyota ~~to~~

~~intercept~~intercepting and record~~ing~~ a copy for access by third parties such as Berla and law enforcement without authorization.

~~62~~

V. CLASS ALLEGATIONS

124. Plaintiffs bring this action as a class action pursuant to Civil Rule 23 on behalf of the following Classes of persons:

> All persons, who within three years prior to the filing of this Complaint, had their text messages and/or call logs intercepted and/or recorded by the infotainment system in a Toyota vehicle (Toyota or Lexus) while a resident of the State of Washington.
>
> Excluded from the Class are Defendant Toyota and any person, firm, trust, corporation, or other entity related to or affiliated with any defendant.

~~63~~125. On information and belief, Toyota vehicles have intercepted and recorded text messages from numerous Washington persons.

~~64~~126. On information and belief, the Class is so numerous that joinder of all affected persons is impracticable and the disposition of their claims in a class action, rather than in individual actions, will benefit both the parties and the courts.

~~65~~127. On information and belief, Class members may be identified from records maintained by one or more of the Washington Department of Licensing, Toyota, and/or Berla, and may be notified of the pendency of this action by mail or electronic mail using the form of notice similar to that customarily used in class actions.

~~66~~128. Plaintiffs' claims are typical of the claims of the other members of the Class.

~~67~~129. All members of the Class have been and/or continue to be similarly affected by Toyota's wrongful conduct as complained of herein. Plaintiffs are unaware of any interests that conflict with or are antagonistic to the interests of the Class.

~~68~~130. Plaintiffs will fairly and adequately protect the Class members' interests and have retained counsel competent and experienced in class actions and complex litigation. Plaintiffs and Plaintiffs~~,~~' counsel will adequately and vigorously litigate this class action, and Plaintiffs are aware of their duties and responsibilities to the Class.

~~69~~131. Toyota has acted with respect to the Class in a manner generally applicable to each Class member. Common questions of law and fact exist as to all Class members and predominate over any questions affecting individual Class members. The questions of law and fact common to the Class include, *inter alia*:

a. Whether Toyota intercepted and/ or recorded private communications and conversations without the consent of all participants in the communication and conversations;

b. Whether Toyota violated RCW 9.73.060; and

~~b~~c. The remedies available to Plaintiffs and the Class.

~~70~~132. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all Class members is impracticable. Furthermore, as the statutory damages suffered by individual Class members is relatively small, the expense and burden of individual litigation makes it impossible as a practical matter for Class members to individually redress the wrongs done to them. There will be no difficulty in managing this action as a class action.

~~71~~133. Toyota has acted on grounds generally applicable to the entire Class with respect to the matters complained of herein, thereby making appropriate the relief sought herein with respect to the Class as a whole.

VI. CAUSES OF ACTION

~~E~~A. First Cause of Action: Washington Privacy Act

~~72~~134. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

~~73~~135. This First Cause of Action is brought pursuant to the Washington Privacy Act, Chapter ~~9.73~~9.73 RCW, on behalf of the Class, against Toyota.

~~74~~136. As to each Plaintiff and member of the Class, Toyota intercepted and recorded private communications transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state of Washington by means of a device designed to record or transmit said communication.

~~75~~137. As to each Plaintiff and member of the Class, Toyota did not first obtain the consent of all the participants in such communications.

~~76~~138. Toyota recorded private conversations by means of a device designed to record or transmit such conversation without first obtaining the consent of all the persons engaged in the conversation.

~~77~~139. Toyota is therefore liable to each Plaintiff and member of the Class for liquidated damages computed at the rate of one hundred dollars a day for each day of violation, not to exceed one thousand dollars for each Plaintiff and member of the Class, and a reasonable attorneys' fee and other costs of litigation, as provided by RCW 9.73.060.

~~78~~140. Toyota's acts and practices in violation of Chapter 9.73 RCW as complained of herein have injured the persons of Plaintiffs and each member of the Class.

~~79~~141. Because Toyota's wrongful interception, recordation and retention of text messages and call logs as alleged above has occurred on more than ten separate occasions and/ or continued for more than ten days, Plaintiffs are entitled to $1,000 of statutory liquidated damages.

~~80~~142. Each member of the Class is therefore entitled to $1,000 of statutory liquidated damages.

~~81~~143. Plaintiff therefore seeks recovery of ~~damages, including specifically~~ statutory damages, on his own behalf and on behalf of each member of the Class, together with the costs of the suit, including reasonable attorneys' fees and other costs of litigation.

~~F~~B. Second Cause of Action: Declaratory Relief

~~82 Plaintiff~~144. Plaintiffs hereby incorporate~~s~~ by reference the allegations contained in the preceding paragraphs of this Complaint.

~~83~~145. This Second Cause of Action is brought pursuant to the Uniform Declaratory Judgments Act, Chapter ~~7247~~7.24 RCW, on behalf of the Class, against Toyota.

~~84~~146. Plaintiffs seek a declaration that Toyota's conduct violates the Washington Privacy Act .

~~G~~C. Third Cause of Action: Injunctive Relief

~~85~~147. Plaintiff hereby incorporates by reference the allegations contained in the preceding paragraphs of this Complaint.

~~86~~148. Plaintiffs seek an injunction from this Court, enjoining Toyota from further interception and recordation of text messages and call logs by use of its infotainment systems, and ordering Toyota to cause its infotainment systems to delete all stored text messages and call logs.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class prays for relief and judgment as follows:

A. Declaring that this action is properly maintainable as a class action under Civil Rule 23, and certifying Plaintiffs as the Class representative and their counsel as Counsel for the Class;

B. Declaring that Toyota intercepted and recorded private communications and conversations in violation of the Washington Privacy Act;

C. Awarding Plaintiffs and the members of the Class~~es~~ the remedy of liquidated damages at the rate of one hundred dollars a day for each day of violation, not to exceed one thousand dollars per Plaintiff and Class member, and a reasonable attorneys' fee and other costs ~~of~~litigation~~of~~ of litigation;

D. Enjoining further violations of the WPA; and

Such other and further relief as this Court may deem just and proper.

VIII. JURY DEMAND

Plaintiffs and the Class hereby demand a trial by jury.

~~///~~

~~///~~

~~August 9, 2021.~~

Document comparison by Workshare 10.0 on Thursday, November 11, 2021 11:13:10 PM

Input:	
Document 1 ID	file://\\perkinscoie\All\Groupdata\Document_Processing\CSM\CS0132093\WIP\Goussev Complaint EDITABLE.docx
Description	Goussev Complaint EDITABLE
Document 2 ID	file://\\perkinscoie\All\Groupdata\Document_Processing\CSM\CS0132093\WIP\2021-11-04 GOUSSEV AMENDED COMPLAINT - CRO annotations.docx
Description	2021-11-04 GOUSSEV AMENDED COMPLAINT - CRO annotations
Rendering set	Perkins

Legend:	
Insertion	
~~Deletion~~	
~~Moved from~~	
Moved to	
Style change	
Format change	
~~Moved deletion~~	
Inserted cell	
Deleted cell	
Moved cell	
Split/Merged cell	
Padding cell	

Statistics:	
	Count
Insertions	315
Deletions	152
Moved from	7
Moved to	7
Style change	0

Format changed	0
Total changes	481